

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-067399
(43)Date of publication of application : 16.03.2001

(51)Int.CI.

G06F 17/60
G06F 19/00
G06T 7/00
G07D 9/00
H04M 3/42
H04M 11/00
H04M 15/00

(21)Application number : 11-237667

(71)Applicant : OKI ELECTRIC IND CO LTD

(22)Date of filing : 25.08.1999

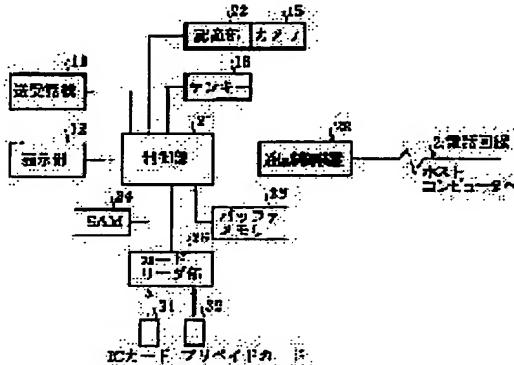
(72)Inventor : TAKIZAWA TOSHIRO

(54) ELECTRONIC MONEY TRANSACTION SYSTEM

(57)Abstract

PROBLEM TO BE SOLVED: To load the electronic money by means of a general telephone circuit.

SOLUTION: In this electronic money transaction system, the irises of an operator of a public telephone set are photographed by a camera 15 and recognized at a recognition part 22. Meanwhile, the personal information stored in an IC card 31 is read at a card reader part 26. The card 31 stores the registered two iris data and a control part 21 compares these iris data with each other to authenticate the identity of the operator. When this identity is authenticated, the loaded amount of electronic money is inputted to generate the communication data including the loaded amount. The communication data are enciphered and then transmitted to a host computer via a telephone circuit 2.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2001-67399

(P 2001-67399 A)

(43) 公開日 平成13年3月16日 (2001. 3. 16)

(51) Int. C.I.⁷

識別記号

F I

テマコード (参考)

G 06 F 17/60

G 06 F 15/21 3 4 0 Z 3E040

19/00

G 07 D 9/00 4 6 1 A 5B043

G 06 T 7/00

H 04 M 3/42 Z 5B049

G 07 D 9/00 4 6 1

11/00 3 0 2 5B055

H 04 M 3/42

15/00 Z 5K024

審査請求 未請求 請求項の数 9

OL

(全 12 頁) 最終頁に続く

(21) 出願番号

特願平11-237667

(71) 出願人 000000295

沖電気工業株式会社

(22) 出願日

平成11年8月25日 (1999. 8. 25)

東京都港区虎ノ門1丁目7番12号

(72) 発明者 滝沢 俊男

東京都港区虎ノ門1丁目7番12号 沖電気工業株式会社内

(74) 代理人 100082050

弁理士 佐藤 幸男

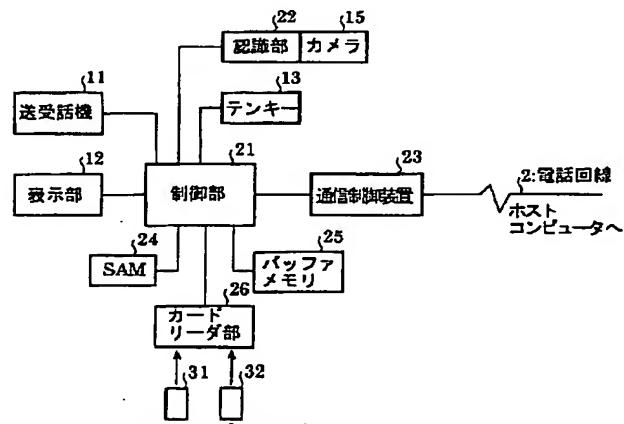
最終頁に続く

(54) 【発明の名称】電子マネー取引システム

(57) 【要約】

【課題】一般の電話回線2を用いて電子マネーのローディングを行う。

【解決手段】公衆電話機の操作者の目のアイリス(虹彩)をカメラ15により撮影し、認識部22で認識する。また、ICカード31に格納されている個人情報をカードリーダ部26を用いて読み取る。このICカード31には、登録されたアイリスデータが格納されており、制御部21では、この2つのアイリスデータを比較して本人認証を行う。本人を認証できたときは、電子マネーのロード金額を入力し、このロード金額を含めて通信データを生成し、暗号化した後、電話回線2を介してホストコンピュータへ送信する。



具体例1の構成を示すブロック図

【特許請求の範囲】

【請求項1】 金融機関の取引対象者が操作する端末と金融機関のホストコンピュータとの間で、通信回線を介して電子マネーによる取引を行う電子マネー取引システムにおいて、

前記通信回線に電話回線を用いるとともに、情報の読み書きが可能なものであって中央演算装置及び記憶手段を内蔵したICカードに、取引対象者のバイオメトリクス情報を登録する一方、

前記端末は、ICカードの真偽を判定するICカード認証手段と、

該ICカード認証手段によりICカードが真と判定されたとき、ICカードに格納されている情報を読み取る情報読み取り手段と、

端末を操作して取引要求を行った操作者から、当該操作者のバイオメトリクス情報を取得するバイオメトリクス情報取得手段と、

前記バイオメトリクス情報取得手段によって取得されたバイオメトリクス情報と情報読み取り手段によって読み出された情報のうちのバイオメトリクス情報を比較して、端末の操作者がICカードに登録された取引対象者本人であるか否かを認証する本人認証手段と、

該本人認証手段により、取引対象者本人であることが認証されたとき、電子マネーによる取引を受け付けて取引要求情報を入力する取引要求情報入力手段と、

該取引要求情報入力手段によって入力された取引要求情報を含む情報に対し、セキュリティ処理を行って通信データを生成し、電話回線を介して該通信データをホストコンピュータに送信する端末側送信手段と、

送信した通信データに対応してホストコンピュータから返信データが返信されたとき、該返信データから取引の処理結果を示す取引処理情報を取り出す端末側受信手段と、を備え、

前記ホストコンピュータは、端末からの通信データを受信して該通信データから取引要求情報を取り出すホスト側受信手段と、

該ホスト側受信手段により取り出された取引要求情報に基づいて取引に関する処理を行う取引処理手段と、

該取引処理手段によって処理されて出力された取引処理結果を含む情報に対し、セキュリティ処理を行って返信データを生成し、通信データの送信元端末に、電話回線を介して該返信データを送信するホスト側送信手段と、を備えたことを特徴とする電子マネー取引システム。

【請求項2】 前記バイオメトリクス情報は、取引対象者及び操作者の目の虹彩画像の情報であることを特徴とする請求項1に記載の電子マネー取引システム。

【請求項3】 前記ICカードに接続先ホストコンピュータの電話番号を記録し、前記端末の情報読み取り手段は、ICカードから当該電話番号を読み取り、端末側送信手段は、読み取られた電話番号に基づいて接続先ホス

10

20

30

40

50

トコンピュータに接続し、通信データを送信するように構成されたことを特徴とする請求項1又は請求項2に記載の電子マネー取引システム。

【請求項4】 前記ICカード及びホストコンピュータに、それぞれ対応する通信用暗号鍵及び通信用復号鍵を格納する一方、

前記端末の情報読み取り手段は、ICカードから通信用暗号鍵を読み取り、端末側送信手段は、セキュリティ処理として、ICカードから読み取った通信用暗号鍵を用いて情報の暗号化を行い、前記端末側受信手段は、ICカードから読み取った復号鍵を用いてホストコンピュータから送信された返信データの復号化を行うように構成され、

前記ホストコンピュータのホスト側受信手段は、セキュリティ処理として、格納された通信用復号鍵を用いて端末から送信された通信データの復号化を行い、前記ホスト側送信手段は、格納された通信用暗号鍵を用いて情報の暗号化を行うように構成されたことを特徴とする請求項1～請求項3のいずれか1つに記載の電子マネー取引システム。

【請求項5】 前記ICカードに、ICカード固有のカードIDを格納し、前記端末の情報読み取り手段は、当該カードIDを読み取り、読み取ったカードIDを用いてICカードに格納された通信用暗号鍵及び通信用復号鍵を読み取るように構成されたことを特徴とする請求項4に記載の電子マネー取引システム。

【請求項6】 前記カードIDは暗号化されたものであることを特徴とする請求項5に記載の電子マネー取引システム。

【請求項7】 前記ホストコンピュータは、暗号化されたカードIDを復号化するカードID復号鍵を格納する一方、

前記端末の端末側送信手段は、暗号化されたカードIDを通信データに含めてホストコンピュータに送信するように構成され、

前記ホスト側受信手段は、通信データから暗号化されたカードIDを取り出し、ホストコンピュータに格納されたカードID復号鍵を用いてカードIDの復号化を行い、該復号化されたカードIDを用いてホストコンピュータに格納された通信用復号鍵を取り出すように構成され、

前記ホスト側送信手段は、ホスト側受信手段によって復号化されたカードIDを用いてホストコンピュータに格納された通信用暗号鍵を取り出すように構成されたことを特徴とする請求項6に記載の電子マネー取引システム。

【請求項8】 前記端末は、公衆電話機であることを特徴とする請求項1～請求項7のいずれか1つに記載の電子マネー取引システム。

【請求項9】 前記端末は、パーソナルコンピュータで

あることを特徴とする請求項1～請求項7のいずれか1つに記載の電子マネー取引システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ICカード、バイオメトリクス情報をを利用してオフラインで認証を行い、電話回線を介して電子マネーの取引を行う電子マネー取引システムに関する。

【0002】

【従来の技術】従来の電子マネー取引システムでは、不正を防止するため、暗証番号を用いて取引対象者の本人認証を行うようにしている。

【0003】しかし、この暗証番号を用いたシステムにおいて、セキュリティ性を向上させるためには、ハードウェア、ソフトウェアを含めてシステム上、高価なものになってしまふ。そこで、近年、本人特有のバイオメトリクス情報を用いて本人認証を行うシステムが開発されている。

【0004】

【発明が解決しようとする課題】しかしながら、このようなバイオメトリクス情報を用いて本人認証を行う従来の電子マネー取引システムにおいても、セキュリティ性を高めるためには、専用の回線を用いて電子マネーのローディングを行う必要があり、いつでもどこでもかかるローディングを手軽に行うというわけにはいかず、通信コストも低減させることは困難であった。従って、一般的の電話回線を用いて電子マネーのローディングを行えるようになれば、容易に電子マネーによる取引を行えるようになる。

【0005】

【課題を解決するための手段】本発明は以上の点を解決するため次の構成を採用する。

〈構成1〉請求項1の発明に係る電子マネー取引システムは、金融機関の取引対象者が操作する端末と金融機関のホストコンピュータとの間で、通信回線を介して電子マネーによる取引を行う電子マネー取引システムにおいて、前記通信回線に電話回線を用いるとともに、情報の読み書きが可能なものであって中央演算装置及び記憶手段を内蔵したICカードに、取引対象者のバイオメトリクス情報を登録する一方、前記端末が、ICカードの真偽を判定するICカード認証手段と、該ICカード認証手段によりICカードが真と判定されたとき、ICカードに格納されている情報を読み取る情報読み取り手段と、端末を操作して取引要求を行った操作者から、当該操作者のバイオメトリクス情報を取得するバイオメトリクス情報取得手段と、前記バイオメトリクス情報取得手段によって取得されたバイオメトリクス情報と情報読み取り手段によって読み出された情報のうちのバイオメトリクス情報とを比較して、端末の操作者がICカードに登録された取引対象者本人であるか否かを認証する本人

認証手段と、該本人認証手段により、取引対象者本人であることが認証されたとき、電子マネーによる取引を受け付けて取引要求情報を入力する取引要求情報入力手段と、該取引要求情報入力手段によって入力された取引要求情報を含む情報に対し、セキュリティ処理を行って通信データを生成し、電話回線を介して該通信データをホストコンピュータに送信する端末側送信手段と、送信した通信データに対応してホストコンピュータから返信データが返信されたとき、該返信データから取引の処理結果を示す取引処理情報を取り出す端末側受信手段と、を備え、前記ホストコンピュータが、端末からの通信データを受信して該通信データから取引要求情報を取り出すホスト側受信手段と、該ホスト側受信手段により取り出された取引要求情報に基づいて取引に関する処理を行う取引処理手段と、該取引処理手段によって処理されて出力された取引処理結果を含む情報に対し、セキュリティ処理を行って返信データを生成し、通信データの送信元端末に、電話回線を介して該返信データを送信するホスト側送信手段と、を備えたものである。

【0006】〈構成2〉請求項2の発明に係る電子マネー取引システムでは、前記バイオメトリクス情報が取引対象者及び操作者の目の虹彩画像の情報である。

【0007】〈構成3〉請求項3の発明に係る電子マネー取引システムでは、前記ICカードに接続先ホストコンピュータの電話番号を記録し、前記端末の情報読み取り手段が、ICカードから当該電話番号を読み取り、端末側送信手段が、読み取られた電話番号に基づいて接続先ホストコンピュータに接続し、通信データを送信するように構成されている。

【0008】〈構成4〉請求項4の発明に係る電子マネー取引システムでは、前記ICカード及びホストコンピュータに、それぞれ対応する通信用暗号鍵及び通信用復号鍵を格納する一方、前記端末の情報読み取り手段が、ICカードから通信用暗号鍵を読み取り、端末側送信手段が、セキュリティ処理として、ICカードから読み取った通信用暗号鍵を用いて情報の暗号化を行い、前記端末側受信手段が、ICカードから読み取った復号鍵を用いてホストコンピュータから送信された返信データの復号化を行うように構成され、前記ホストコンピュータのホスト側受信手段が、セキュリティ処理として、格納された通信用復号鍵を用いて端末から送信された通信データの復号化を行い、前記ホスト側送信手段が、格納された通信用暗号鍵を用いて情報の暗号化を行うように構成されている。

【0009】〈構成5〉請求項5の発明に係る電子マネー取引システムでは、前記ICカードに、ICカード固有のカードIDを格納し、前記端末の情報読み取り手段が、当該カードIDを読み取り、読み取ったカードIDを用いてICカードに格納された通信用暗号鍵及び通信用復号鍵を読み取るように構成されている。

【0010】〈構成6〉請求項6の発明に係る電子マネー取引システムでは、前記カードIDが暗号化されたものである。

【0011】〈構成7〉請求項7の発明に係る電子マネー取引システムでは、前記ホストコンピュータが、暗号化されたカードIDを復号化するカードID復号鍵を格納する一方、前記端末の端末側送信手段が、暗号化されたカードIDを通信データに含めてホストコンピュータに送信するように構成され、前記ホスト側受信手段が、通信データから暗号化されたカードIDを取り出し、ホストコンピュータに格納されたカードID復号鍵を用いてカードIDの復号化を行い、該復号化されたカードIDを用いてホストコンピュータに格納された通信用復号鍵を取り出すように構成され、前記ホスト側送信手段が、ホスト側受信手段によって復号化されたカードIDを用いてホストコンピュータに格納された通信用暗号鍵を取り出すように構成されている。

【0012】〈構成8〉請求項8の発明に係る電子マネー取引システムでは、前記端末が公衆電話機である。

【0013】〈構成9〉請求項9の発明に係る電子マネー取引システムでは、前記端末がパーソナルコンピュータである。

【0014】

【発明の実施の形態】以下、本発明の実施の形態を具体例を用いて説明する。

〈具体例1〉具体例1は、ICカードを用い、通信回線として電話回線を用いて端末としての公衆電話機から電子マネーのローディングを行うようにしたものである。

【0015】図1は、具体例1の構成を示すブロック図であり、図2は、図1の構成を内蔵した公衆電話機1の外観を示す斜視図である。図2に示すように、公衆電話機1の側面には送受話器11が備えられ、前面パネルには、表示部12、テンキー13、ICカード挿入口14及びレシート排出口16が配置されている。

【0016】テンキー13は、例えば12個のキーを備え、相手の電話番号及び電子マネーのロード金額を入力するのに使用する取引要求情報入力手段である。表示部12は、例えば液晶を用いた表示部であり、文字のほか、イメージも表示できるものである。

【0017】この表示部12の上部には、バイオメトリクス情報取得手段としてのカメラ15が配置されている。このカメラ15は、CCD(charge coupled device: 電荷結合素子)を備え、操作者の目を撮影してバイオメトリクス情報としての虹彩(アイリス)の画像を得るためのものである。

【0018】虹彩は眼球の角膜と水晶体との間にあり、中央に瞳孔を有する薄膜である。この虹彩は、瞳孔の開閉をコントロールして眼球内に入る光の量を調節するものであり、幼年期に完成され、各人毎によって異なるパターンを有している。このパターンは右目と左目とでも

10

20

30

40

50

相違するが、一生を通じてほとんど変化することはない。従って、虹彩の情報は、まさに本人しか保有できない有力なバイオメトリクス情報となる。

【0019】尚、バイオメトリクス情報としては、虹彩に限られるものではなく、サイン、網膜、声紋、顔貌、指紋、手形の情報を用いることもできる。サイン、声紋、顔貌、指紋、手形の情報を用いるときは、カメラ15の代わりに、これらの情報を得ることのできるバイオメトリクス情報取得手段を用いる。但し、この虹彩パターンを用いれば、サインや指紋、声紋等と比較して少ないデータ量で本人認証を行うことができるので、有利である。レシート排出口16はレシートを排出する出口であるが、これはオプションである。

【0020】図3は、具体例1のシステム構成図である。ネットワーク3は、銀行5のホストコンピュータが接続されたネットワークであり、ネットワーク4は、カード会社6のコンピュータが接続されたネットワークである。公衆電話機1は電話回線2、ネットワーク3を介して銀行5のホストコンピュータに、さらにネットワーク4を介してカード会社6のホストコンピュータに接続されている。そして、銀行カード決済のときは、公衆電話機1と銀行5のホストコンピュータとの間で電子マネーのローディングが行われ、クレジットカード決済のときは、公衆電話機1とカード会社6のホストコンピュータとの間で電子マネーのローディングが行われる。

【0021】この公衆電話機1は、図1に示すように、制御部21と、通信制御装置23と、認識部22と、SAM(Security Application Module)24と、バッファメモリ25と、カードリーダ部26とを内蔵している。

【0022】制御部21は、マイクロコンピュータ、周辺ROM、RAM、I/Oとのインターフェース等を備えて構成され、送受話器11、表示部12、テンキー13等もこの制御部21に接続されている。そして、制御部21は、公衆電話機1を制御し、後述するフローチャートに従って電子マネーのロードを実行する。

【0023】認識部22は、カメラ15と接続され、カメラ15によって捕らえられた操作者の目の画像に基づいて、目の虹彩(アイリス)の画像のデジタルデータを作成し、このデジタルデータを一旦蓄積し、このデータと別のデータとで本人であるかどうかの認証処理を行うためのものである。

【0024】SAM24は、ICカード31の真偽を認証するために使用するICカード認証手段であり、ICカード31とほぼ同一の構成を有している。通信用のバッファメモリ25は、送受信する情報を一旦ストアしておくためのものである。

【0025】通信制御装置23は、モデム/NCU等を備え、通信制御を行なう装置であり、電話回線2、ISDN回線を経由して銀行5又はカード会社6のホストコン

ピュータに接続される。

【0026】カードリーダ部26は、ICカード31、例えばテレホンカードのようなプリペイドカードを受け付けて、データをリードライトする情報読み取り手段である。尚、プリペイドカードはオプションである。

【0027】ICカード31は、そのカード基材にIC(集積回路)チップを埋め込んで構成されたカードであり、このICカード31に取引対象者本人の個人情報が記録される。このICカード31のICチップには、CPU(中央演算装置)、各種処理プログラムが書き込まれたROM(Read Only Memory)、取引内容等を一時的に記憶するためのRAM(Random Access Memory)、電気的に記憶情報の消去、書き込みが可能な不揮発性メモリであるEEPROM(Electrically Erasable and Programmable ROM)が設けられている。さらにこのICチップには、データを記憶させるための記憶回路、そして、これらの各メモリの情報の読み取り、書き込みを制御する制御回路も一体に形成されている。このICカード31の表面には、ICチップに接続された端子部が露出し、この端子部を介して情報の読み書きが行われる。尚、近年、ISO10536やISO14443に公開されているように、接触部のないICカードも開発されており、このような非接触型ICカードでも同様に用いることができる。

【0028】図4は具体例1のICカード31のファイル構成を示す説明図である。ICカード31に格納されたファイルは階層化され、マスタファイルの下に複数の専用ファイルがあり、さらにその下にエレメンタリファイルがある。このエレメンタリファイル1には、カードID、個人名、アイリストデータ、暗証番号用暗号鍵、ロード金額、接続電話番号、口座番号、ロード金額復号鍵、カードID復号鍵等の個人情報が記録され、エレメンタリファイル2には、通信用暗号鍵、通信用復号鍵が記録されている。

【0029】尚、カードIDは、通信用暗号鍵、通信用復号鍵の情報を読み取るときに用いる情報であり、セキュリティ性を高めるため、暗号化されている。また、アイリストデータは前述の虹彩パターンに関するデータであり、そのデータサイズは、例えば256バイトである。

【0030】このICカード31は、ICカード31の破損を避けるため、接続端子がICカード挿入口14の端子(図示せず)に接続されるまで、非活性化され、データの読み書きができないようになっている。このICカード31にデータの読み書きを行うためには、JIS規格JISX6306に規定されている手順に従ってICカード31を活性化させる必要がある。

【0031】図5は、銀行5又はカード会社6のホストコンピュータの構成を示すブロック図である。ホストコンピュータ41は、ファイル42~44を備えている。ファイル42は、ログ用ファイルであり、ファイル43

は、カードIDの復号鍵を格納したファイルであり、ファイル44は、通信用暗号鍵、通信用復号鍵、暗証番号用復号鍵を格納したファイルである。

【0032】(具体例1の動作)図6及び図7は具体例1の動作を示すフローチャートである。ステップ(図中、「S」と記す。)1では、操作者が、自分のICカード31へ電子マネーを充填するためにICカード31をICカード挿入口14に挿入し、このICカード31を吸い込む。

10 【0033】ステップ2では、SAM24を用いて相互認証を行い、ICカード31の真偽を判定する。相互認証は、ICカードのJIS規格JISX6306に規定されているEXTERNAL AUTHENTICATEコマンド、あるいはINTERNAL AUTHENTICATEコマンドを使い、暗号技術を用いて行われる。EXTERNAL AUTHENTICATEコマンドは、ICカード31外部で暗号化し、ICカード31内で認証結果を計算させるときに用いられるコマンドであり、INTERNAL AUTHENTICATEコマンドは、外部から種となる情報、例えば乱数を与えて暗号化し、その認証結果を外部で判断するときに用いられるコマンドである。相互認証中、公衆電話機1の表示部12にメッセージが表示される。

【0034】図8は、表示部12に表示するメッセージの表示例を示す説明図である。この図8(A)に示すように、相互認証中、表示部12には「カード認証中」「しばらくお待ち下さい」とのメッセージが表示される。そして、カードが真と認証されたときは、ステップ3に進む。ステップ3では、カメラ15を用いて操作者の目を撮影し、操作者のアイリスト画像を取り込む。

【0035】このとき、図8(B)に示すように、「あなたの確認を致します。」「矢印の先のレンズをご覧下さい」とのメッセージを表示させ、操作者の注意を引くようにする。そして、できるだけ目線を表示部12に集中させるため、矢印を点滅等させる。認識部22は、取り込んだアイリスト画像をデジタルデータに変換し、256バイトのアイリストデータを得る。

【0036】ステップ4では、ICカード31から、登録されているアイリストデータを読み取る。読み取りは、40 カードリーダ部26によって行われる。このアイリストデータは、図4に示すようにエレメンタリファイルに格納されている。

【0037】ステップ5では、カメラ15から取り込んだアイリストデータとICカード31から読み取ったアイリストデータとを比較して本人の認識を行う。このアイリスト認証には、例えば米国特許第5,291,560号公報に開示された技術を用いる。本人を認証できたときは、ステップ8に進む。

【0038】また、本人を認証できなかったときはステップ6に進み、所定のリトライ回数、例えば3回以下で

あるか否かを判定する。リトライ回数が3回以下のときは、ステップ3に戻り、再び本人の認証を行う。このとき、表示部12に、もう一度操作者に本人の認証を行う旨のメッセージを表示させる。

【0039】リトライ回数が3回以下で本人を認証できたときは、ステップ8に進む。また、リトライ回数が3回を超えたときは、操作者は、取引対象者本人ではないと判定してステップ7に進み、取引の停止処理を行う。このとき、操作者に暗証番号を入力させ、確認するようにもよい。暗証番号が入力されたときは、ICカード31に格納されている暗証番号用暗号鍵を用いて暗号化される。

【0040】ステップ8では、ICカード31に対し、READコマンドを発行し、ICカード31のエレメンタリファイル1に格納されている個人情報等及びエレメンタリファイル2に格納されている通信用暗号鍵、通信用復号鍵を直接読み取る。尚、通信用暗号鍵、通信用復号鍵を直接読み取ることはできず、カードIDが必要である。また、このカードIDは暗号化されているため、これらの鍵情報を読み取るには、まず、エレメンタリファイル1からカードID復号鍵を取り出して、このカードIDを復号化する。そして、この復号化されたカードIDを用いてエレメンタリファイル2に格納されている通信用暗号鍵、通信用復号鍵を読み取る。このようにしてセキュリティ性を高めている。

【0041】ステップ9では、読み取った個人情報をバッファメモリ25に格納する。ステップ10では、図8(C)に示すように、「ロード金額を入力して下さい」とのメッセージを表示部12に表示させ、操作者に取引要求情報としてロード金額の入力を促す。操作者は、このメッセージに従ってテンキー13を用い、所定のロード金額を入力する。ステップ11では、入力されたロード金額をバッファメモリ25に格納し、通信データを生成する。

【0042】図9は、具体例1の前半の動作を示す動作説明図である。この図9(A)に示すように、この通信データには、カードID、口座番号、ロード要求金額、暗証番号、アイリストデータ等が含まれ、この先頭部にヘッダ、後端にはエンドデータが付加される。

【0043】ステップ12では、図9(B)に示すように、バッファメモリ25に格納された通信データのうち、口座番号、ロード要求金額、暗証番号、アイリストデータ等のデータを暗号化する。尚、暗証番号は、ステップ7において入力されるオプションデータであり、暗証番号があるときは、二重に暗号化されることになる。これによってセキュリティ性が高められる。

【0044】この暗号化は、ICカード31から読み取られた通信用暗号鍵を用いて行われる。暗号方式としては共通鍵方式のDES(Data Encryption Standard)、公開鍵方式のRSA等を用いるのが一般的であるが、こ

の方式に限られるものではない。

【0045】ステップ13では、ICカード31から読み取った接続電話番号を用いてホストコンピュータ41に接続し、この通信データを送信する。但し、テンキー13を用いて接続先ホストコンピュータの電話番号を入力することもできる。

【0046】ステップ14～16は、ホストコンピュータ41によって実行される。ステップ14では、図9(C)に示すように、受信した通信データを復号化する。

【0047】通信データを復号化するには、まず、暗号化されたカードIDを通信データから取り出し、このカードIDを、ファイル43に格納されているカードIDの復号鍵を用いて復号化する。そして、復号化されたカードIDの番号をキーとしてファイル44を検索し、ファイル44から通信用復号鍵と暗証番号用復号鍵を取り出す。さらに、この通信用復号鍵を用いて通信データを復号化する。尚、暗号化された暗証番号が含まれているときは、暗証番号用復号鍵を用いてこの暗証番号を復号化する。

【0048】このように公衆電話機1から送信されたカードIDを用いてファイル44から通信用復号鍵と暗証番号用復号鍵を取り出すようにしたので、このカードIDを分からなければこれらの復号鍵を取り出すことができず、セキュリティ性が保証される。

【0049】ステップ15では、ホストコンピュータ41が所定の処理を行う。図10は、具体例1の後半の動作を示す動作説明図である。このホストコンピュータ41の処理により、図10(A)に示すように、復号化された通信データから口座番号とロード要求金額が取り出され、口座番号に基づいて電子マネーが引き出される。処理終了後、口座番号、ロード金額及びアイリストデータはログ用のファイル42へ記録され、トランザクションが残る。トランザクションを残すことにより、確実に口座を有する取引対象者本人に対して金額をロードしたという証拠が残る。

【0050】ステップ16では、図10(B)に示すように、カードID、口座番号及びロード金額が格納された通信データを形成し、ファイル44から取り出された通信用暗号鍵を用いてこの口座番号とロード金額を暗号化し、図10(C)に示すような通信データを生成する。尚、この通信用暗号鍵は、前述の復号化したカードIDの番号をキーとして取り出される。生成された通信データは、送信元の公衆電話機1に送信され、公衆電話機1は、ステップ17～19を実行する。

【0051】ステップ17では、図10(D)に示すように、通信データを受信し、ICカード31から読み取った通信用復号鍵を用いて復号化する。その結果、図10(E)に示すような通信データが得られる。そして、WRITEコマンドを発行し、この通信データに格納さ

れているロード金額情報を、ICカード31のエレメンタリファイルのロード金額エリアに格納する。

【0052】ステップ18では、図8(D)に示すように、「ありがとうございました」とのメッセージを表示させるとともに、取引日付、口座番号、ロード金額、取引通番を表示部12の画面に表示させる。表示後、ICカード31を非活性化させるとともに、ICカード31をICカード挿入口14からリリースする。

【0053】ステップ19では、結果をレシートに印刷し、このレシートをレシート排出口16から排出する。尚、ステップ5が本人認証手段に、ステップ12及び13が端末側送信手段に、ステップ14がホスト側受信手段に、ステップ15が取引処理手段に、ステップ16がホスト側送信手段に、ステップ17が端末側受信手段に相当する。

【0054】〈具体例1の効果〉以上、説明したように具体例1によれば、端末として公衆電話機1を利用し、電話回線2を用いて電子マネーのローディングを行うようにしたので、一般の電話回線2が接続された公衆電話機1があれば、専用の回線を用いることなくいつでもどこでも通信できる。このため、通信コストを低減することができる。

【0055】また、ICカード31を用いてオフラインで本人認証を行い、電子マネーをロードするようにしたので、ホスト側に負荷をかけずに本人認証を行うことができ、しかも安全に電子マネーをロードすることができる。また、本人特有のアイリストデータを用いて電子マネーをロードするようにしたので、本人以外の他人によって電子マネーを引き出すという不正行為を防止することができ、セキュリティ上、万全なシステムを構築することができる。

【0056】また、ICカード31から通信用暗号鍵、復号鍵を読み取り、この2つの鍵を用いて通信データの暗号化、ホストコンピュータ41からの返信データの復号化を行い、さらに、このカードIDを用いて2つの鍵を読み取るとともに、このカードIDも暗号化するようにしたので、一般的の電話回線2を用いた場合でも安全に通信を行うことができる。

【0057】また、この暗号化されたカードIDをホストコンピュータ41に送信し、このカードIDを復号化し、このカードIDを用いてファイル44から通信用暗号鍵等を取り出すようにして、このカードIDを知らない第三者によって簡単に通信用暗号鍵等を取り出せないようにしたので、セキュリティ性が向上する。

【0058】また、公衆電話機1からホストコンピュータ41に通信データを送信するとき、ICカード31から読み取った接続電話番号を用いて自動的にホストコンピュータ41に接続するようにしたので、操作者の負担を低減することができる。

【0059】さらに、ホストコンピュータ41側では、

口座から引き落とす処理を行う場合に、操作者のアイリストデータを登録してトランザクションを残すようにしたので、本人が電子マネーのロードを行ったという証拠を残すことができ、万が一、犯罪等が発生したときに、その解決に役立てることができる。

【0060】尚、本具体例1では、ステップ7において、暗証番号をオプションとして入力するようにしたが、暗証番号を入力させ、アイリストデータと暗証番号とを併用して本人認証を行うようにしてもよい。また、この暗証番号については、二重に暗号化するようにしたが、セキュリティ性が保証されれば、暗証番号用暗号鍵による暗号化を省略することもできる。

【0061】〈具体例2〉具体例2は、端末としてパーソナルコンピュータを用い、このパーソナルコンピュータに電話回線を接続し、パーソナルコンピュータから電子マネーのローディングを行うようにしたものである。

【0062】図11は、具体例2の構成を示すブロック図であり、図12は、図11の構成を備えたシステムの外観を示す説明図である。図12に示すように、パーソナルコンピュータ51は、例えば液晶表示のディスプレイ52と、キーボード53とを備え、さらにディスプレイ52の上部にカメラ54を備えたノート型のパーソナルコンピュータである。

【0063】このパーソナルコンピュータ51には、所定のデータを入力するためのマウス55と、ICカード31へのデータの読み書きを行うためのICカードリーダライタ56と、電話回線2とが接続されている。

【0064】図11に示すように、ディスプレイ52、マウス55、キーボード53は、制御部21に接続されている。具体例2では、SAM24がICカードリーダライタ56に内蔵されている。尚、具体例1と同一要素については同一符号を付して説明を省略する。

【0065】〈動作〉パーソナルコンピュータ51を用いて電子マネーのローディングを行うときは、ICカード31をICカードリーダライタ56に挿入する。挿入後、ICカード31とICカードリーダライタ56に内蔵されたSAM24との間で相互認証が行われる。そして、具体例1と同じように電子マネーのローディングが行われる。

【0066】〈具体例2の効果〉以上、説明したように具体例2によれば、汎用性のあるパーソナルコンピュータ51を利用して電子マネーのローディングを行うようにしたので、電話回線2があれば、家庭でもオフィスでもいつでもどこでも手軽に、電子マネーのロードを行うことができる。

【0067】尚、本具体例2では、ノート型のパーソナルコンピュータを利用した場合について説明したが、これに限られるものではなく、スタンドアローン型のパーソナルコンピュータを利用することもできる。

【図面の簡単な説明】

13

【図1】本発明の具体例1の構成を示すブロック図である。

【図2】具体例1の公衆電話機の外観を示す斜視図である。

【図3】具体例1のシステム構成図である。

【図4】具体例1のICカード31のファイル構成を示す説明図である。

【図5】ホストコンピュータの構成を示すブロック図である。

【図6】具体例1の動作を示すフローチャート(その1)である。

【図7】具体例1の動作を示すフローチャート(その2)である。

【図8】表示部に表示するメッセージの表示例を示す説明図である。

14

【図9】具体例1の動作説明図(その1)である。

【図10】具体例1の動作説明図(その2)である。

【図11】具体例2の構成を示すブロック図である。

【図12】具体例2のシステムの外観を示す説明図である。

【符号の説明】

1 公衆電話機

2 電話回線

15、54 カメラ

21 制御部

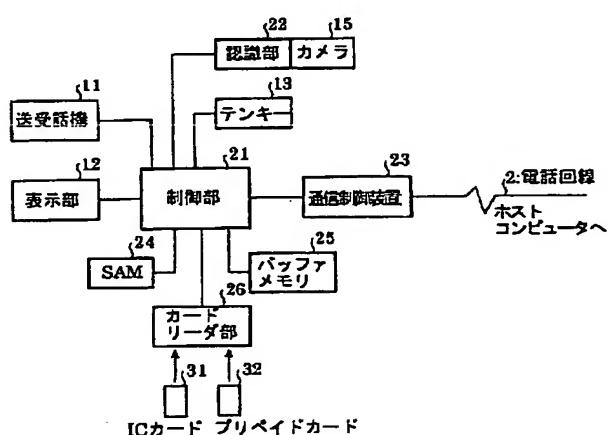
22 認識部

41 ホストコンピュータ

51 パーソナルコンピュータ

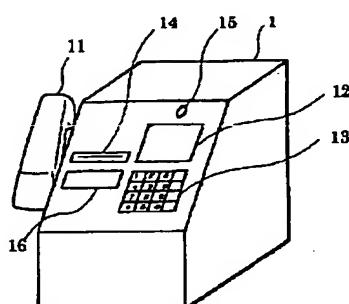
56 ICカードリーダライタ

【図1】



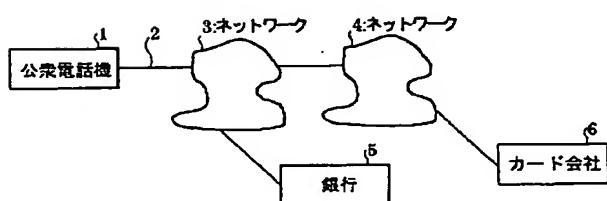
具体例1の構成を示すブロック図

【図2】



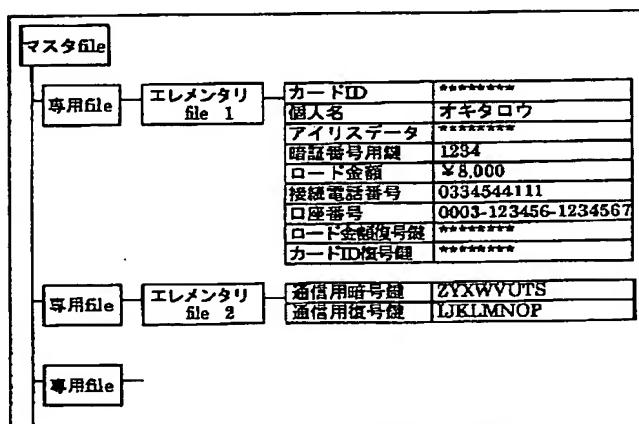
具体例1の公衆電話機の外観を示す斜視図

【図3】



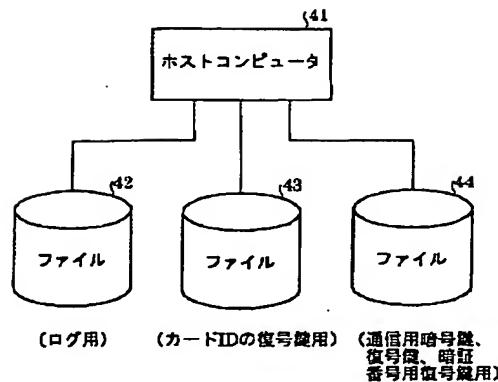
具体例1のシステム構成図

【図4】



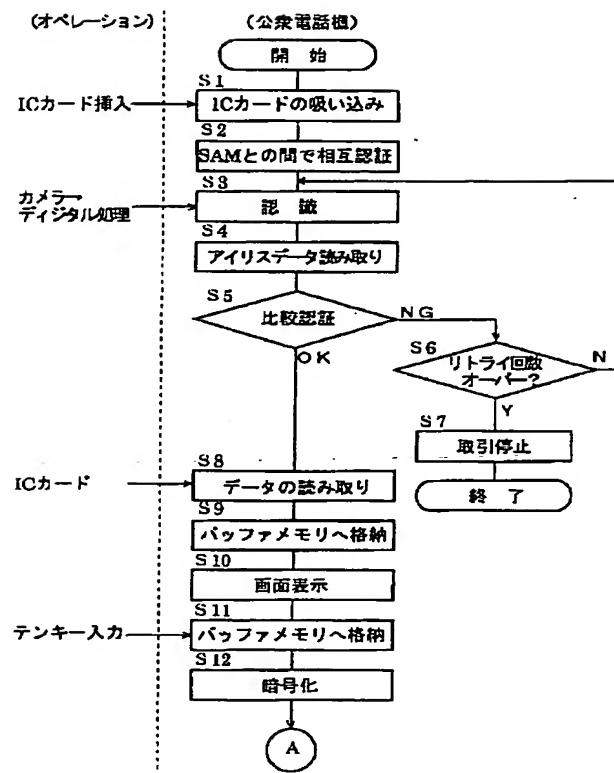
具体例1のICカードのファイル構成を示す説明図

【図5】



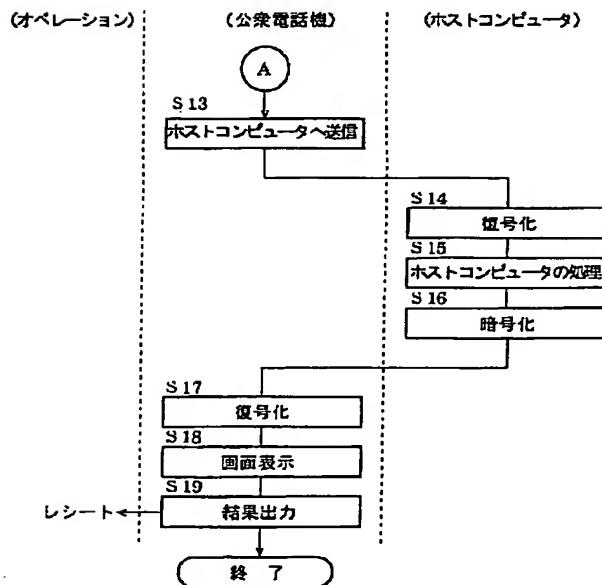
具体例1のホストコンピュータの構成を示すブロック図

【図6】



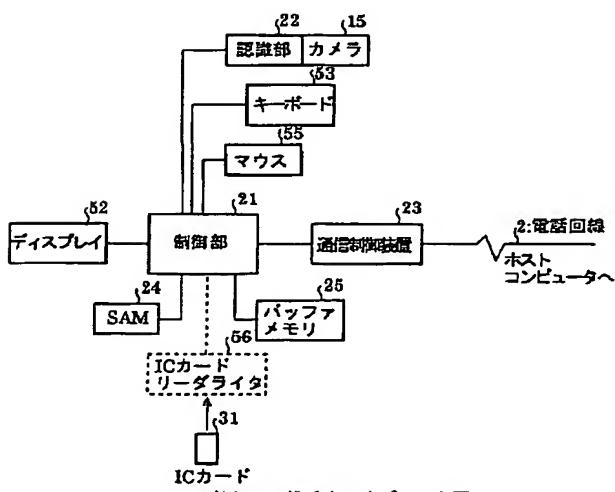
具体例1の動作を示すフローチャート（その1）

【図7】



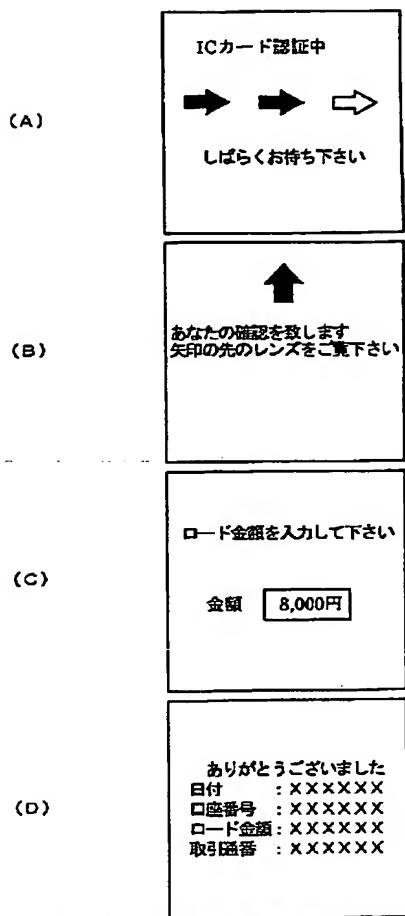
具体例1の動作を示すフローチャート（その2）

【図11】



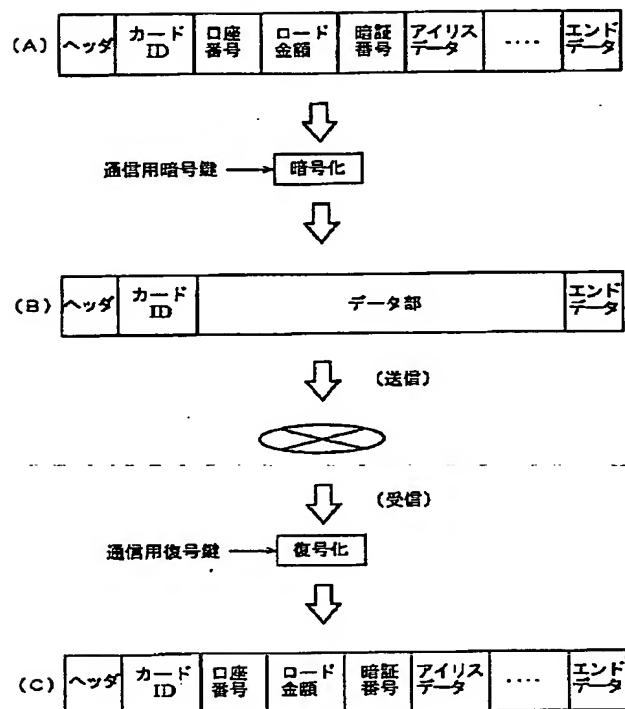
具体例2の構成を示すブロック図

【図8】



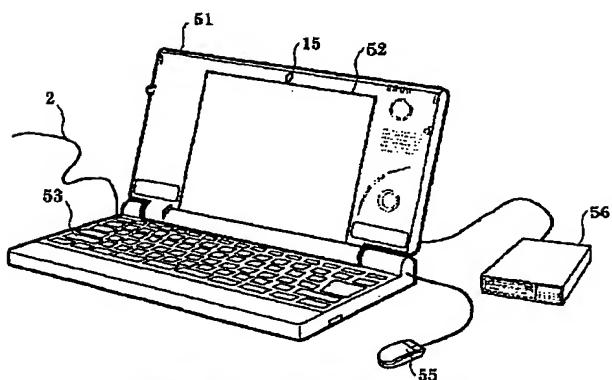
具体例1の公衆電話機の表示部に表示するメッセージの説明図

【図9】



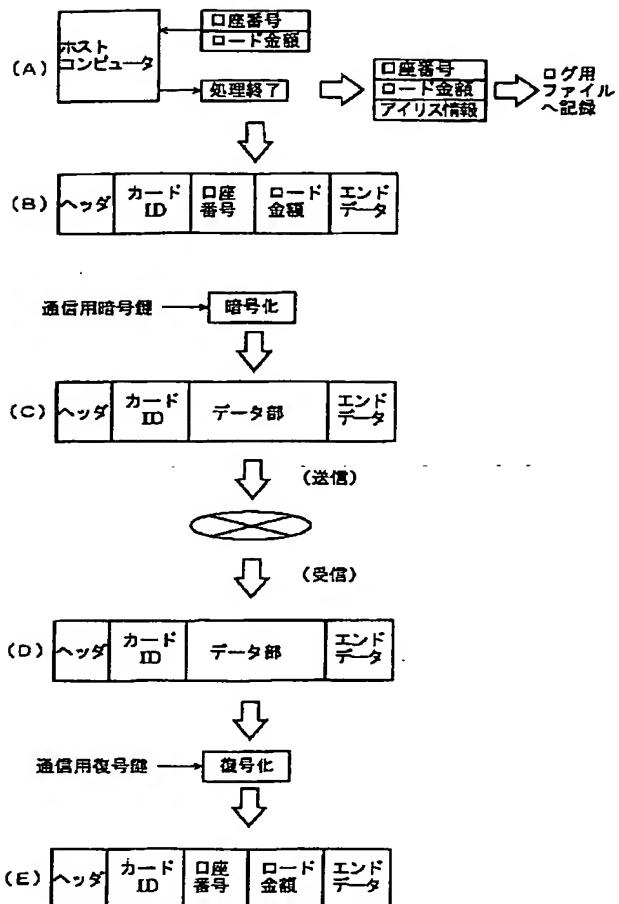
具体例1の動作説明図（その1）

【図12】



具体例2のシステムの外観を示す斜視図

【図10】



具体例1の動作説明図(その2)

フロントページの続き

(51) Int. Cl. 7	識別記号	F I	テマコード(参考)
H 04 M 11/00	302	G 06 F 15/30	M 5K025
15/00			C 5K101
			340 9A001
			350A
		15/62	465K

Fターム(参考) 3E040 AA03 CA11 CB04 DA02 DA10
FH05 FK09
5B043 AA01 AA09 BA04 CA10 DA05
FA04
5B049 AA05 BB46 CC39 DD04 EE10
EE22 EE23 FF08 GG02 GG04
GG07 GG10
5B055 BB12 BB16 CB09 EE02 EE12
EE17 EE21 EE27 FA05 HB02
HB03 HB04 JJ05 KK05 KK09
KK19 MM18 PA05 PA22 PA33
PA34 PA36
5K024 DD06 GG05
5K025 DD07
5K101 NN05 PP04
9A001 BB02 BB03 BB04 BB05 CC02
DD09 EE03 HH21 HH23 JJ08
JJ12 JJ66 JJ67 KK57 KK58
LL03